Controlling Powerful Levels of System Access

Commonwealth of Massachusetts

Chief Fiscal Officer Conference

November 18th, 2008

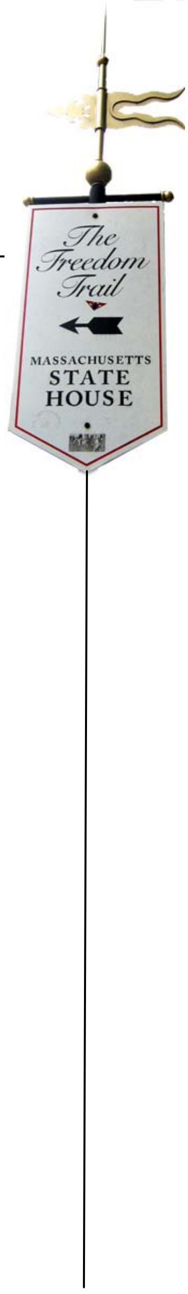
KPMG LLP

Controlling Powerful System Access

Automated systems can streamline operations and make an organization more efficient **but** they increase risk that must be managed.

- Multiple enterprise applications in state government
- Powerful access is necessary in some situations
- Management oversight is key to maintaining control
- Certification forces management to review periodically
- Goal: balance access and risk management

Managing System Access

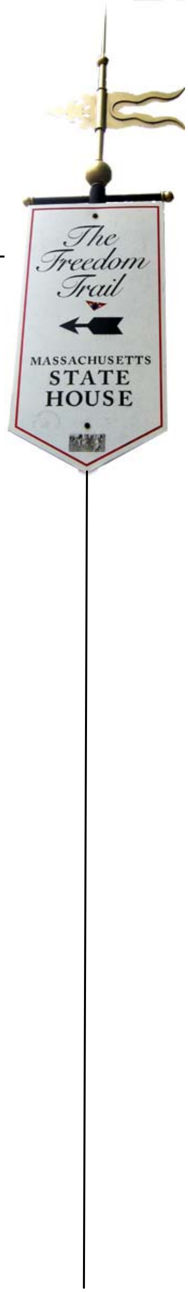


Managing system access is a shared responsibility:

- Department Security Officer (DSO)
- Chief Financial Officer (CFO)
- Payroll Director
- Department Head

Massachusetts Policies

- Enterprise system security policy issued last fiscal year
- Certification required twice a year
  - Department Head during open/close
  - DSO at the end of calendar year
- Access to department as well as enterprise systems is needed to assure appropriate use of sensitive data as well as financial resources



This Session

Goal: Review current practices and findings from the field

Best Practices and Current Trends:

Glenn Siriano, Partner in charge of the KPMG Northeast Information Protection Practice

Peter Scavotto, Director of Quality Assurance Bureau, CTR

Approaches to Resolving Department Challenges: panel discussion with frequently asked questions as well as issues raised by you

Defining “Appropriate Access”

Many legal and regulatory requirements require organizations to define and apply “appropriate access” to systems and data.

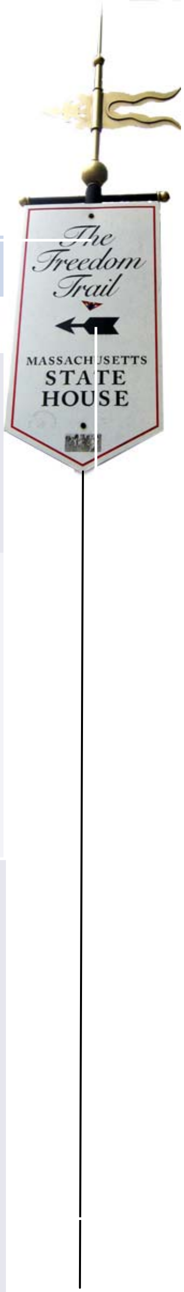
Appropriate Access can be defined in a number of ways:

- the most limited access required for a user to perform his/her responsibilities.
- security that prevents unauthorized or unapproved access to confidential/proprietary information
- one that provides effective controls over key business processes (e.g. segregation of duties)

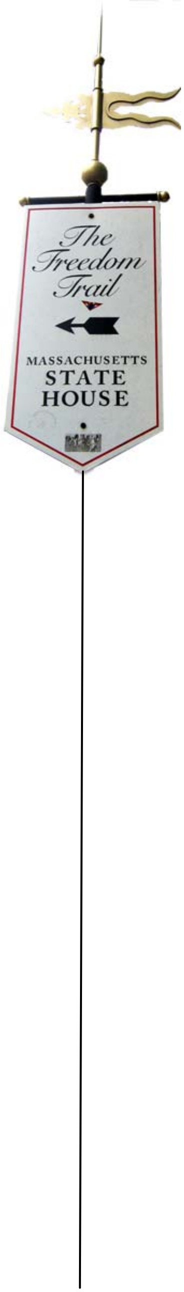
The most effective definition of “appropriate access” is: the level of access to an organization’s information systems and data that most effectively and efficiently allows an employee, customer, or business partner to conduct their business processes while maintaining the organization’s control according to their risk management thresholds.”

Approaches to Defining Roles

	Pros	Cons
Top-Down	Easy to implement and Involves various managers and supervisors upfront to determine Roles for their users.	Time consuming and involves many iterations as the managers are not aware about the actual access held by their users.
Bottom-Up	Roles are more comprehensive and have actual access related to the Role.	Managers/Supervisors do not take ownership when not involved. Does not provide information on job duties to managers to make intelligent decisions on Roles.
Hybrid	Comprehensive Roles are developed with underlying access that needs to be provided as part of Role. Involves the managers up-front and provides the intelligence on the actual access held by the users and their job responsibilities.	Time consuming and cumbersome if done manually.



Challenges of Defining Appropriate Access



Appropriate access can be difficult to model in today’s organizations:

- Department consolidations and shared services can change the nature of what is appropriate.
- Developing or terminating programs or initiatives may change requirements for access.
- A user who changes jobs or roles within an organization may have more access than appropriate.

Creating a very rigid or formalized definition of appropriate access can generate significant rework when a “change event” occurs. An appropriate access program tied closely to the organization’s risk management program and enabled by technology will create the most flexible framework.

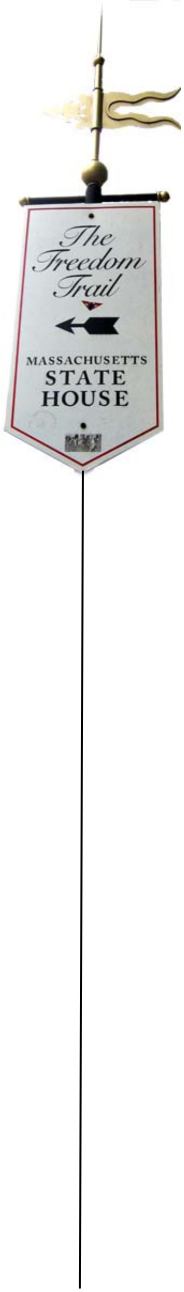
Role Management – KPMG's Observations

Creating Roles, organization must guard against:

- Optimistic view on required starting points:
  - —Lack of clear job descriptions
  - —Lack of (up-to-date) authorization matrices
  - —Lack of commitment of the organization to support appropriate roles.

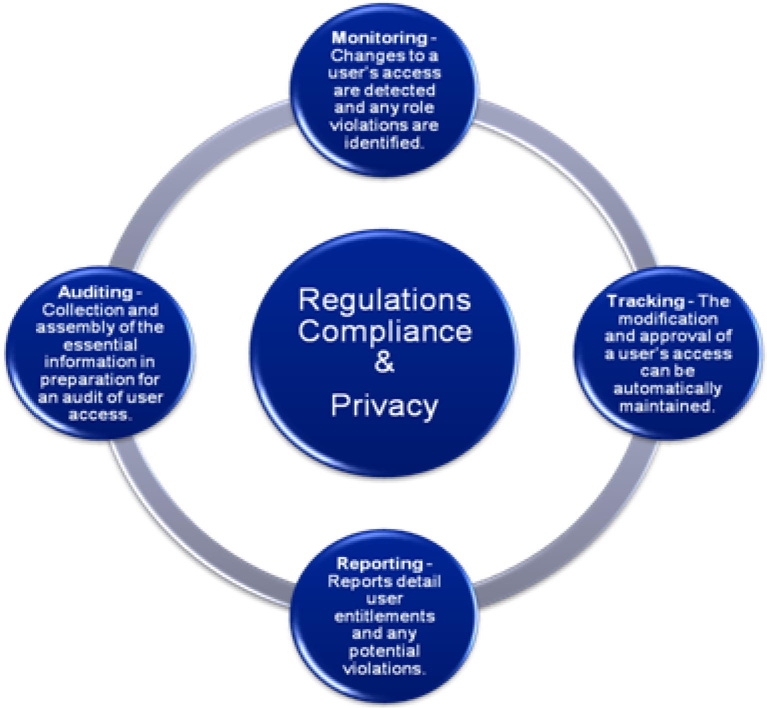
- Theoretical/conceptual view leading to role explosion:
  - —Top-down approach may take too long and require too much effort and interaction with the business
  - —No room for flexibility may lead to inappropriate user behavior
  - —Difficulty assuring roles address future needs.

- Too ambitious an approach can lead to revolution instead of evolution:
  - —Big bang: scope is entire organization and all applications – is this feasible?
  - —Phased approach is crucial.



Access Certification

- Crucial that the appropriateness of roles be reviewed and validated
- Provides assurance to management that user access is appropriate across applications and restricted according to their job responsibility
- Assures implementation of roles reflect segregation of duties and assists with maintenance of roles



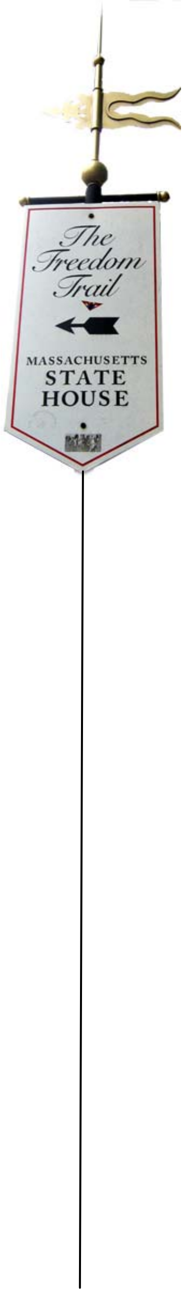
Regulations Compliance & Privacy

Monitoring - Changes to a user's access are detected and any role violations are identified.

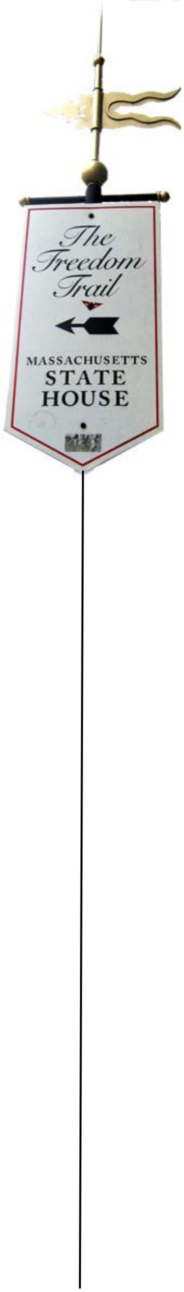
Tracking - The modification and approval of a user's access can be automatically maintained.

Reporting - Reports detail user entitlements and any potential violations.

Auditing - Collection and assembly of the essential information in preparation for an audit of user access.



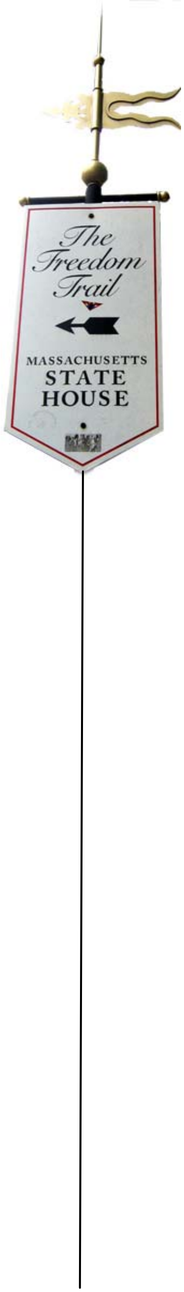
Approach to Reviewing Access



A number of factors impact the breadth and approach to evaluating appropriate access. Organizations should inventory systems and summarize the risk and existing controls, focusing on:

- Primary applications
- Current processes for requesting and certifying access privileges
- Classification of data in application (e.g., financial, private, or confidential)
- Financial impact of the application
- Effectiveness of network controls within and surrounding the application (e.g., network access, physical security, operational controls)

Access Certification: KPMG’s Observations



Scope

Organizations continue to struggle with managing the scope of reviews:

- A high volume of in-scope applications
- A high volume of user privileges under review
- The number of open audit issues

Organizations are starting to implement a risk-based approach to performing reviews:

- Manage the impact to individual process owners performing the reviews
- Structuring reviews with different frequencies factoring each application’s individual risk.

Access Certification: KPMG's Observations

Methods: Organizations continue to focus on improving the process:

- Increase preventive controls, roles and responsibilities, etc.
- Education and Awareness training for User Managers.

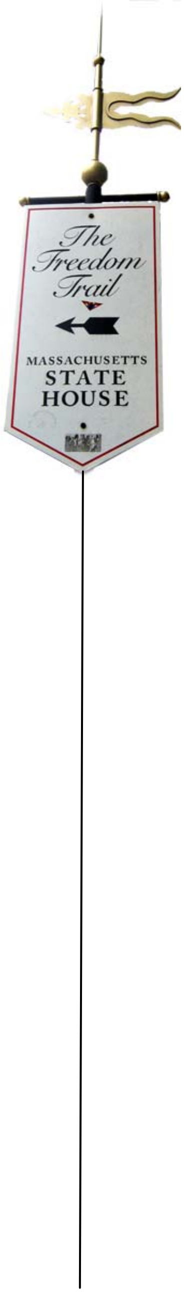
Automation is not yet mature:

- Widespread use of homegrown applications
- Data quality issues is a foundational component.

There appears to be an opportunity to integrate IAM *What is IAM?* solutions to business applications.

What are others doing (Based on Financial Services Companies)

Does your organization make decisions regarding granting access on risk factors?	66% - Yes
Do you classify information resources based on risk?	**79% - Yes**
Do you classify roles based on risk?	**51% - Yes**
What types of applications do you consider most at risk?	**51% - Business unit specific applications**
What is the process for assigning access rights today?	**30% - An ‘ad-hoc’ process; 30% - through non-central, but well defined processes**
How often does an employee or contractor have too much access?	**35% - Sometimes; 29% - Often**



***Ponemon Institute Preliminary Report - February 2nd, 2008**

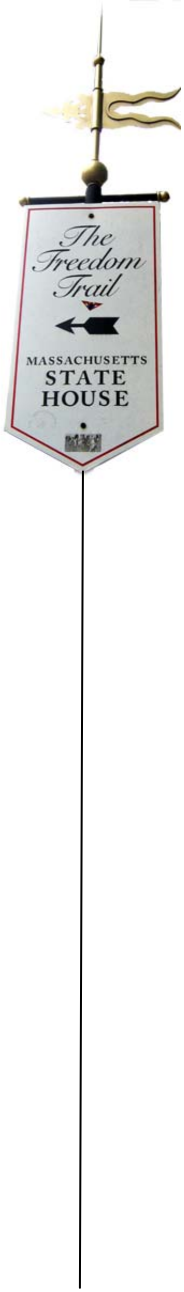
What are others doing (Based on Financial Services Companies)

How is access granted to an employee or contractor?	28% - On department and title; 25% - On request basis
What process is used for granting access?	**43% - Homegrown access control solutions;** **30% - Automated solution (off the shelf)**

What process is used to certify access?	**39% - Manual process;**
	26% - Homegrown system;
	17% - Automated solution (off the shelf)

How does your organization control privileged users' access to information resources and/or systems?	**42% - combination of technology and manually-based identity management controls** **25% - technology-based identity management controls**
How will the importance of access governance change in your organization in the next two years?	**47% - become more important** **42% - stay the same in terms of importance**

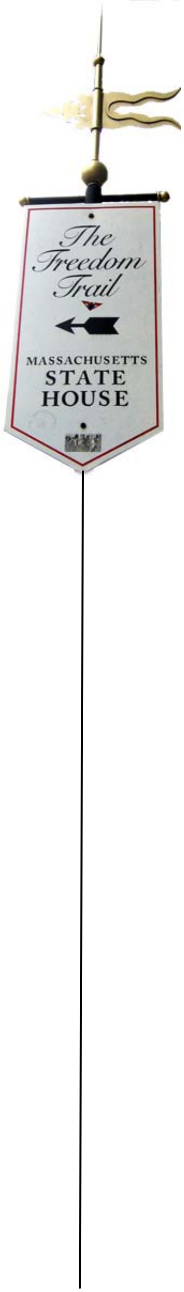
***Ponemon Institute Preliminary Report - February 2nd, 2008**



Some Practical Advice:

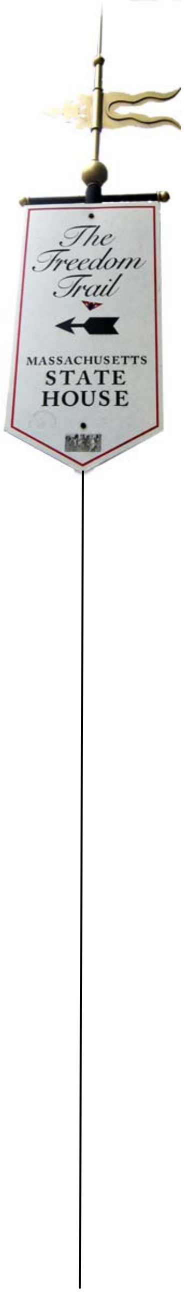
- Limit the most powerful access (administrator rights) to the minimum number of people needed to support the department
- Log the most powerful access rights and powerful combinations and monitor usage
- Analyze roles to understand your risk points
- Define appropriate access based on a flexible, high-level model that can adapt to change
- Implement Role Modeling in a phased approach – based on risk

Audits in General



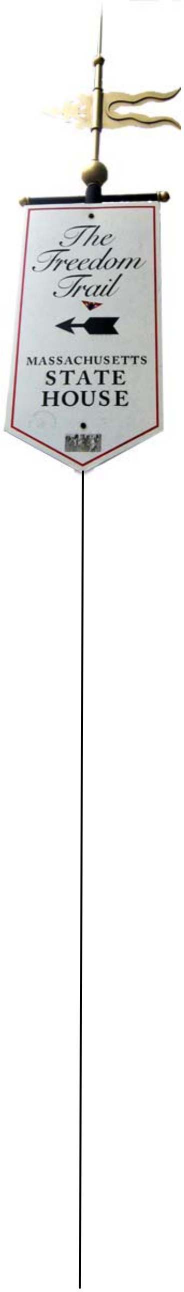
Quality Assurance Visits

- Test of controls vs. substitute for controls
- Verify compliance
  - State finance law
  - Comptroller policies and regulations



How are we Received?

Is Your Sense of Security . . . FALSE?



- …if all risks are not well managed — from the mailroom to the boardroom — and if
- there is nothing in place to ensure the system of internal control is strong throughout the enterprise, your organization has no safety net.
-
- **THE INSTITUTE OF INTERNAL AUDITORS**
- Issue 29 M

TONE at the TOP

What Should be in Place

- Department – Wide Internal Control Plan
- Tone at the Top
    - Soft controls – expectations of behavior
- Objectives – all functional areas
- Risk Assessment – all functional areas
- Mitigate risk – hard controls
- Communication
- Monitoring/Testing of controls

What Should be in Place

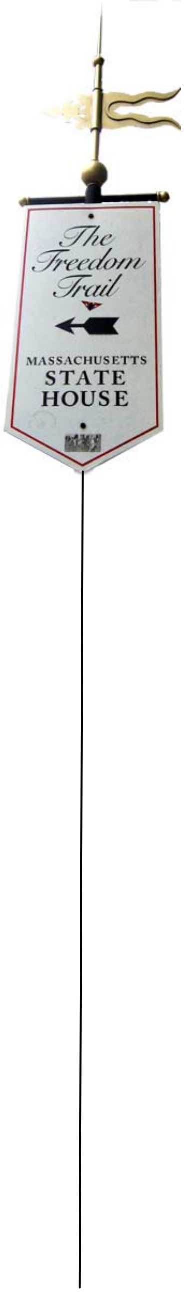
Security Plan

- Risk Assessment
  - Transactions used are based on your business

    Revenue, payments, interfaces, labor distribution
- Segregation of duties
- Enterprise systems
  - HRCMS, e*mpac
  - MMARS
  - CIW
- Department systems
  - Writing and moving code
  - Client application – processing vs. approval

What Should be in Place

- Hard controls
  - Security roles
  - Internal limits - $ threshold, access by region
  - Updating profiles
  - Deleting access on separation from service or change in roles
- Monitor
  - DocDirect security reports
  - Query UAID activity
  - Wet signatures



What We Look For - Security

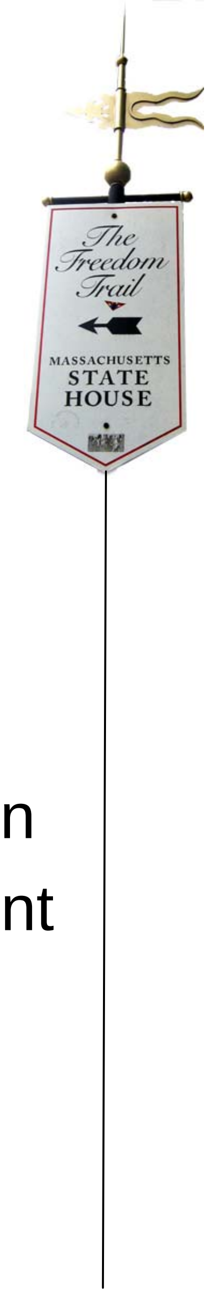
(CNN)

What We Look For - Security

- Segregation of duties
- Additional departmental limits on security
- Evidence of DHSA
- Use of powerful roles
  - DFISC
  - Payment and encumbrance +/or vendor

What We Find

- Signature Authorization
  - DHSA but no UAID indicator
  - No DHSA at all
  - DHSA from another department
- UAIDs – MMARS access remains after ITD inactivation
- Single user creates/submits encumbrance and payment



When We Leave

LEVELS OF SYSTEM ACCESS AND POTENTIAL RISKS

(State of Oregon)

System Access	Action Allowed	Potential Risk
Create transactions	The user records data and documents the transaction.	The data created is: Incorrect, Fraudulent Used for unintended purposes.
Data inquiry	The user is given access to "view" data only.	The data is disclosed to unauthorized individuals. Data is used for unintended purposes.
Modify transactions	The user changes existing data.	The integrity of the data is compromised, thereby affecting the reliability of the data for its intended purpose.
Delete transactions	The user temporarily or permanently destroys data.	The data is not available to the system owner and other authorized users. Information cannot be reconciled.
Submit transactions	Transactions finalized - go to done/complete status.	Submitted without approval. Submitted by creator, no SOD.

Other Potential Risks

System Access	Action Allowed	Potential Risk
Limited to top management	Approval.	Work not processed on time. Client benefits delayed.
Limited to a few staff	Create/submit.	Late payments to vendors. Discounts missed. Employee works before hired. Employee paid after termination.
Limited to technical staff	Warehouse reports.	Information unavailable when needed.